COMMUNICATION TECHNIQUE	N° TC1422	Ed. 02
OmniPCX Enterprise/OmniPCX Office	Nb de pages : 19	Date : 07-07-2011

☐ URGENTE

■ NON URGENTE ☐ TEMPORAIRE ■ DEFINITIVE

OBJET : EXEMPLE DE CONFIGURATION DU SWITCH OMNI ACCESS WIRELESS EN VERSION 5.X

SOMMAIRE

1. INTRODUCTION 2
2. TOPOLOGIE 3
3. CONFIGURATION INITIALE 4
3.1 Assistant de configuration 4
3.2 VLAN et adresse IP 5
3.3 Mise à jour logicielle 6
3.4 Ajout de licences 7
3.5 Redémarrage du switch 7
4. CONFIGURATION DES PARAMETRES WLAN 8
4.1 QoS WLAN 8
4.1.1 Profil SSID 8
4.1.2 Profils EDCA 9
4.1.3 Profil Call Access Control (CAC) profile 9
4.1.4 QOS pour prioritisation de la VoIP 9
4.2 Sécurité WLAN 10
4.2.1 Profil d'authentification AAA 10
4.2.2 Application Layer Gateway (ALG) Noe 10
4.2.3 Sécurité avec licence PEFNG 10
4.2.4 Création du rôle 11
4.2.5 Attribution du rôle 11
4.2.6 Firewall session-idle-timeout 11
4.3 AP virtuel 11
4.4 Groupe d'AP 12
4.5 Proxy ARP 12
4.6 Configuration Radio 12
4.6.1 Utilisation de la radio 802.11a par les postes WLAN 12
4.6.2 ARM – Adaptive Radio Management 13
4.6.3 ARM et Basic & Transmit rates optimisation 14
4.6.4 Paramétrage des fréquences Radio 15
5. CONFIGURATION DES POINTS D'ACCES 16
5.1 Configuration du serveur DHCP de l'OAW 16
5.2 Réinitialisation d'un AP 17
6. RAPPEL SUR LA QOS DES OMNIPCX 18
6.1 Configuration OmniPCX Office 18
6.2 Configuration OmniPCX Enterprise 19
7. AVERTISSEMENT 19

1. INTRODUCTION

La version 5.0.3.x du switch OmniAccess Wireless (OAW) apporte des améliorations pour les réseaux distants :

- Réservation de bande passante RAP,
- Accès RAP local des clients,
- Portail Mesh distant

Ainsi qu'un nouveau modèle de licence:

- Licences MAP et VPN sont intégrées dans l'OS de base
- La licence RAP est intégrée dans la licence AP
- La licence PEF (par utilisateur) est convertie en PEF Nouvelle Génération (par AP).

Cette release AOS inclut le support de nouveaux AP additionnels pour les topologies WLAN.

Cette communication technique décrit la configuration de l'OAW nécessaire au bon fonctionnement de la solution IP Touch 310/610 WLAN et OmniTouch 8118/8128 WLAN dans une topologie sans serveur SVP. Les topologies avec serveurs SVP, si ceux-ci doivent être conservés, les topologies multi-switchs et les topologies spécifiques ne sont pas décrites.

L'exemple de configuration décrit ci-après a été effectué avec la version 5.0.3.0, sur un OmniAccess 4308.

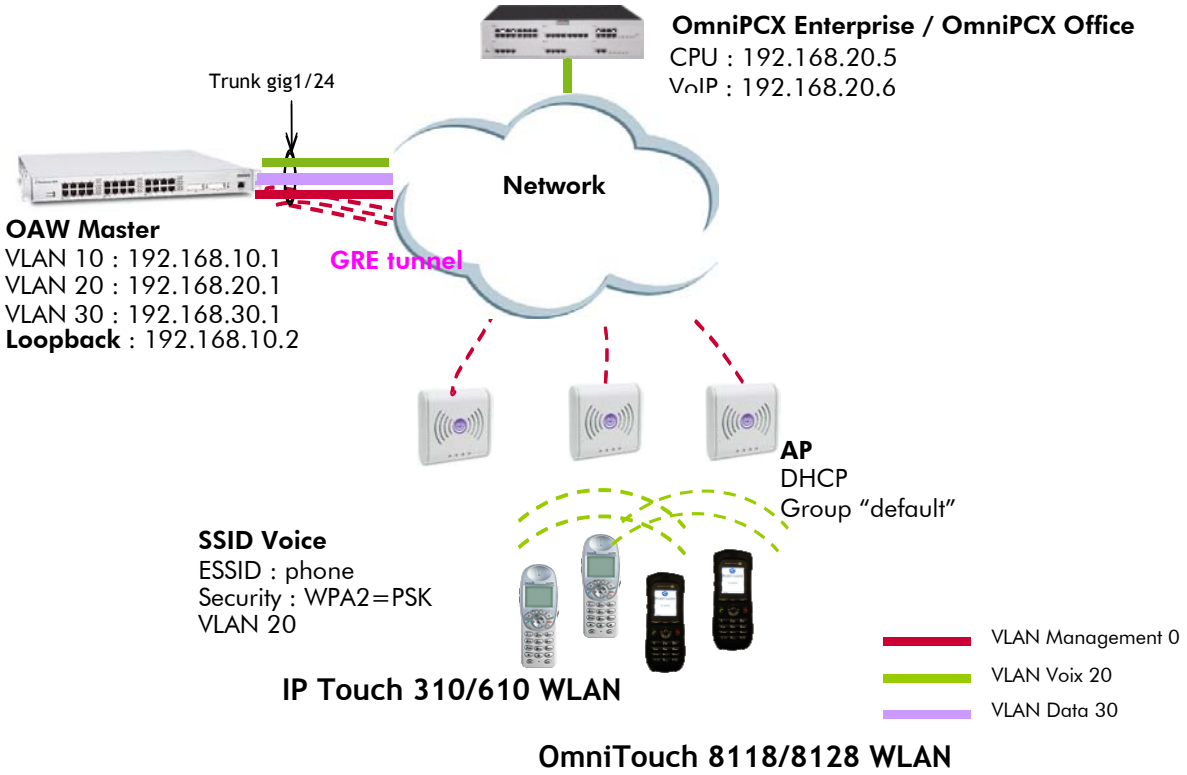
Toutes les fonctionnalités liées à la Voix sont intégrées à la licence **PEFNG** (Policy Enforcement Firewall New Generation) qui est **obligatoire**.

Se reporter également aux communications sur la solution VoWLAN pour connaître les restrictions sur les logiciels utilisés.

2. TOPOLOGIE

La topologie mise en place dans cet exemple est une topologie mono-OAW, c'est-à-dire que tous les APs établissent leur tunnel GRE vers le même contrôleur WLAN.

L'OAW sera configuré dans l'architecture ci-dessous :



Dans cette architecture, 3 VLANs sont utilisés :

- VLAN 10 : appelé VLAN de Management, dans lequel va transiter le flux entre les APs et l'OAW,
- VLAN 20 : appelé VLAN Voix dans lequel se trouvent les téléphones,
- VLAN 30 : appelé VLAN Data pour les PCs sans fil.

Les mobiles IP Touch 310/610 et OmniTouch 8118/8128 WLAN utiliseront le ESSID "phone" en mode WMM Admission Control avec une sécurité WPA2-PSK (chiffrement AES).

3. CONFIGURATION INITIALE

3.1 Assistant de configuration

L'assistant de configuration est affiché au premier démarrage de l'OAW. Il permet de configurer les paramètres obligatoires au démarrage du système : nom, adresse IP, login, mot de passe, etc...

Ces paramètres doivent être configurés en utilisant le câble série (paramètres par défaut 9600-8-1-N). Conserver les valeurs d'adressage IP par défaut : elles seront configurées ultérieurement selon la topologie.

```
Enter System name [OAW-4308]: OAW-Master
Enter VLAN 1 interface IP address [172.16.0.254]:
Enter VLAN 1 interface subnet mask [255.255.255.0]:
Enter IP Default gateway [none]:
Enter Switch Role, (master|local) [master]:
Enter Country code (ISO-3166), <ctrl-I> for supported list: fr
You have chosen Country code FR for France (yes|no)?: yes
Enter Time Zone [PST-8:0]:
Enter Time in GMT [23:03:22]:
Enter Date (MM/DD/YYYY) [12/12/2010]:
Enter Password for admin login (up to 32 chars): *****
Re-type Password for admin login: *****
Enter Password for enable mode (up to 15 chars): ******
Re-type Password for enable mode: ******
Do you wish to shutdown all the ports (yes|no)? [no]:

Current choices are:

System name: OAW-Master
VLAN 1 interface IP address: 172.16.0.254
VLAN 1 interface subnet mask: 255.255.255.0
IP Default gateway: none
Switch Role: master
Country code: fr
Time Zone: PST-8:0
Ports shutdown: no

If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no) yes

Creating configuration... Done.

System will now restart!

Shutdown processing started


The system is going down NOW !!
```

3.2 VLAN et adresse IP

Dans cet exemple, 3 VLANs sont configurés sur l'OAW :

- le premier (VLAN 10) contient tous les équipements réseau : switchs, APs, routeurs, etc.,
- le deuxième (VLAN 20) contient les équipements voix : OmniPCX Enterprise / OmniPCX Office, IP Phones, Mobile IP Touch, OmniTouch etc.,
- le troisième (VLAN 30) contient les équipements data : PC, PDA, etc..

Configuration des 3 VLANs :

```
User: admin
Password: *****
(OAW-Master) >en
Password:******

(OAW-Master) #
(OAW-Master) #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(OAW-Master) (config) #vlan 10
(OAW-Master) (config) #interface vlan 10
(OAW-Master) (config-subif)#ip address 192.168.10.1 255.255.255.0
(OAW-Master) (config-subif)#!
(OAW-Master) (config) #interface loopback
(OAW-Master) (config-loop)#ip address 192.168.10.2
Switch IP Address is Modified. Switch should be rebooted now

(OAW-Master) (config-loop)#!
(OAW-Master) (config) #vlan 20
(OAW-Master) (config) #interface vlan 20
(OAW-Master) (config-subif)#ip address 192.168.20.1 255.255.255.0
(OAW-Master) (config-subif)#!
(OAW-Master) (config) #vlan 30
(OAW-Master) (config) #interface vlan 30
(OAW-Master) (config-subif)#ip address 192.168.30.1 255.255.255.0
(OAW-Master) (config-subif)#!
```

Le port gigabit Ethernet1/8 de l'OAW-4308 véhicule ces VLANs en mode trunk : supprimer l'adresse IP du VLAN 1 qui n'est pas utilisé.

```
(OAW-Master) (config) #interface gigabitethernet 1/8
(OAW-Master) (config-if)#switchport mode trunk
(OAW-Master) (config-if)#switchport trunk allowed vlan add 10,20,30
(OAW-Master) (config-if)#!
(OAW-Master) (config) #interface vlan 1
(OAW-Master) (config-subif)#no ip address
(OAW-Master) (config-subif)#!
```

Note

L'équipement réseau auquel est raccordé l'OAW doit avoir une configuration réseau correspondante.

Si une passerelle par défaut doit être ajoutée, la syntaxe est la suivante :

```
(OAW-Master) (config) #ip default-gateway 192.168.10.254
```

3.3 Mise à jour logicielle

Il est important d'avoir l'OAW à jour avant de commencer la configuration. En effet, certains paramètres ne seront disponibles que dans la dernière version. Cette mise à jour peut se faire par l'interface web (Maintenance -> Image Management) en fournissant le fichier image, par serveur FTP ou serveur TFTP ou par chargement de fichier local.

Dans cet exemple, le serveur TFTP est sur le même VLAN que le switch et utilise l'adresse IP 192.168.10.111. Le logiciel est installé sur la partition 1. Au reboot suivant, cette nouvelle version sera utilisée.

```
User: admin
Password: *****
(OAW-Master) >enable
Password:******
```

La base de données interne change à partir de l'AOS 3.4. A partir d'une configuration existante, il est recommandé de faire une sauvegarde de la configuration pre-3.4 avant la mise à jour en 5.0.

Pour créer le fichier de backup flashbackup.tar.gz:

```
(OAW-Master) #backup flash
Please wait while we tar relevant files from flash...
Please wait while we compress the tar file...
Checking for free space on flash...
Copying file to flash...
File flashbackup.tar.gz created successfully on flash.
Please copy it out of the switch and delete it when done.
```

Puis, mettre à jour la version du switch :

```
(OAW-Master) #copy tftp: 192.168.10.111 OAW4308_5.0.3.0_26207 system: partition 1
(OAW-Master) (config) #copy tftp: 192.168.10.111 OAW4308_5.0.3.0_26207 system:
partition 1
Copying file: ..................................................................
..............................................................................
File copied successfully.
Saving file to flash:
..............................................................................
The system will boot from partition 1 during the next reboot.
```

Pour visualiser les versions installées sur les partitions, taper la commande show image version.

```
(OAW-Master) #show image version
---------------------------------
Partition               : 0:0 (/dev/hda1) **Default boot**
Software Version        : AOS-W 5.0.3.0
Build number            : 26207
Label                   : 26207
Built on                : 2010-11-30 10:27:56 PST
---------------------------------
Partition               : 0:1 (/dev/hda2)
Software Version        : AOS-W 3.4.3.0
Build number            : 25081
Label                   : 25081
Built on                : 2010-08-23 15:58:58 PDT
```

Note: *La mise à jour de l'OAW directement en version 5.0 à partir d'une version 2.5 n'est pas supportée.*

3.4 Ajout de licences

La licence **PEFNG** est obligatoire pour gérer la Qualité de Service sans fil. L'ensemble des mécanismes et protocoles ouverts par cette licence permet de compenser l'absence du serveur SVP.

Avant mise à jour en AOS-W 5.0, vérifier les besoins en termes de licences et installer toute nouvelle licence nécessaire avant l'upgrade vers AOS-W 5.0.

Les licences en AOS-W 5.0 sont consolidées, certains noms de licence et module peuvent être renommés.

Pour ajouter une licence :

```
(OAW-Master) # license add d6rcjmXq-20BxNlym-nz0GqxYJ-u1LG+x5X-7VJEX0Nn-1i8
Please reload the switch for the new service key to take effect.
```

L'ajout de toute licence se fait par la même procédure.

3.5 Redémarrage du switch

Le redémarrage du switch est obligatoire dans certains cas : modification de l'adresse IP système, ajout de licence, mise à jour de la version. Sauvegarder la configuration avant de redémarrer.

```
(OAW-Master) #write memory
Saving Configuration...

Configuration Saved.

(OAW-Master) #reload
Do you really want to reset the system(y/n): y
System will now restart!
```

Une clé partagée (PSK) par défaut permet les communications inter-switch.

Ne pas utiliser cette PSK par défaut même en mode stand-alone (topologie mono-switch). Laisser la PSK à sa valeur par défaut expose le canal IPSec à de sérieux risques.

Pour configurer la PSK sur le switch master:

```
(OAW-Master) #localip 0.0.0.0 ipsec <psk_secret>
```

4. CONFIGURATION DES PARAMETRES WLAN

Le ESSID "phone" est créé pour les mobiles IP Touch 310/610 et OmniTouch 8118/8128 WLAN.

La sécurité choisie est WPA2-PSK (chiffrement AES) et le VLAN utilisé est le VLAN 20.

4.1 QoS WLAN

Les mobiles IP Touch 310/610 et OmniTouch 8118/8128 WLAN supportent le WMM, WMM Power Save et le WMM Admission Control. L'infrastructure WLAN doit également supporter et autoriser chacun de ces mécanismes QoS afin de s'assurer qu'ils sont bien utilisés.

4.1.1 Profil SSID

Le profil SSID "phone" est créé avec les paramètres de QoS WiFi-Standards nécessaires:

- Activation de la qualité de service **wmm** et de l'économie d'énergie **wmm-uapsd**
- Configuration des paramètres DSCP appliqués pour les trafics voix, video, best-effort et background comme configurés sur le PBX: **wmm-XX-dscp**
- Le WMM TSPEC Min inactivity interval positionné à 5 min: **wmm-ts-min-inact-int**
- Activation du préambule court : **short-preamble**
- Le **dtim-period** positionné à 5 (pour une meilleure autonomie du poste),
- Nombre de retransmissions **max-retries** positionné à 4,
- Nombre maximal de clients associés **max-clients** à 25,
- Garder la valeur 0 par défaut du "Maximum Transmit Failures" : **max-tx-fail**
- Choix de la sécurité WPA2-PSK: "WPA2 personal" et encryption "aes" et saisie de la passphrase

```
(OAW-Master) (config) #wlan ssid-profile ssid_phone_wpa2
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #essid phone
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #wmm
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #wmm-uapsd
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #wmm-vi-dscp 26
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #wmm-vo-dscp 46
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #wmm-be-dscp 0
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #wmm-bk-dscp 0
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #wmm-ts-min-inact-int 300000
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #short-preamble
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #no battery-boost
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #dtim-period 5
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #max-retries 2
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #max-clients 25
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #max-tx-fail 0
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #wpa-passphrase 1234567890
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #opmode wpa2-psk-aes
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #!
```

Dans le profil "High-throughput SSID Profile", "High throughput enable" active le 802.11n qui supporte l'encryption "Open" ou WPA2 (PSK ou Enterprise). Désactiver le paramètre "High throughput enable" si une encryption différente est utilisée auquel cas des échecs d'authentification se produiront.

Le 802.11n doit être désactivé sur le poste (non supporté): le choix non-n 802.11b/g ou 802.11a doit être sélectionné manuellement s'il ne l'est pas automatiquement (sélectionné par défaut au démarrage du poste). Utiliser WinPDM pour configurer ce paramètre.

4.1.2 Profils EDCA

Créer et positionner les paramètres EDCA (Enhanced Distributed Control Access) pour les profils AP/Station présents avec le profil SSID.

Configurer l'"acm" vidéo et l'"acm" voix à 1 (0 par défaut).

```
(OAW-Master) (config) #wlan edca-parameters-profile station "EDCA-station"
(OAW-Master) (EDCA Parameters profile (AP) "EDCA-station") #video acm 1
(OAW-Master) (EDCA Parameters profile (AP) "EDCA-station") #voice acm 1
(OAW-Master) (config) #wlan edca-parameters-profile ap "EDCA-ap"
(OAW-Master) (EDCA Parameters profile (AP) "EDCA-ap") #video acm 1
(OAW-Master) (EDCA Parameters profile (AP) "EDCA-ap") #voice acm 1

(OAW-Master) (config) #wlan ssid-profile "ssid_phone_wpa2"
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #edca-parameters-profile station
"EDCA-station"
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #edca-parameters-profile ap "EDCA-ap"
```

4.1.3 Profil Call Access Control (CAC) profile

Le CAC est géré par l'OAW. Il faut déterminer un nombre maximal de postes WLAN en communication simultanément autorisé par AP et par radio.

Dans cet exemple, 7 combinés WLAN sont autorisés en communication. 20% de marge pour les handovers est réservée.

Nombre maximum de communication active = CAC - CAC * Call Handoff Reservation

Si le paramètre "VoIP Call Capacity" est 7, le VoIP Call Handoff Reservation est 20%, sur un AP, seuls 5 postes WLAN peuvent être en communication au même moment. 2 appels sont réservés pour le déplacement des postes vers cet AP.

```
(OAW-Master)(config) #wlan voip-cac-profile default
(OAW-Master)(VoIP Call Admission Control profile "default")#call-admission-control
(OAW-Master)(VoIP Call Admission Control profile "default")#call-capacity 7
(OAW-Master)(VoIP Call Admission Control profile "default")#call-handoff-reservation 20
```

S'assurer que le VoIP TSPEC Enforcement est désactivé.

```
(OAW-Master)(VoIP Call Admission Control profile "default")#no wmm-tspec-enforcement
(OAW-Master)(VoIP Call Admission Control profile "default" #!
```

4.1.4 QOS pour prioritisation de la VoIP

Activer la prioritisation de la voix :

```
(OAW-Master) (config) #voip prioritization enable
```

4.2 Sécurité WLAN

4.2.1 Profil d'authentification AAA

Utiliser le profil d'**authentification dot1x** prédéfini (**default-psk**). Dans ce profil **default-psk**, la valeur par défaut d'intervalle entre 2 échanges de clés WPA doit être diminuée à 100 ms ; la valeur par défaut étant 1 seconde.

```
(OAW-Master) (config) #aaa profile aaa_phone
(OAW-Master) (AAA Profile "aaa_phone") #authentication-dot1x "default-psk"
(OAW-Master) (AAA Profile "aaa_phone") #!
```

```
(OAW-Master) (config) #aaa authentication dot1x "default-psk"
(OAW-Master) (802.1X Authentication Profile "default-psk") #timer wpa-key-period 100
(OAW-Master) (802.1X Authentication Profile "default-psk") #!
```

4.2.2 Application Layer Gateway (ALG) Noe

L'OAW va analyser le flux de signalisation NOE entre les call servers et les postes afin de détecter ceux en cours de communication. Avec la licence **PEF** installée, l'ALG peut également être utilisée pour ouvrir/fermer dynamiquement les ports RTP utilisés par le trafic voix.

Pour visualiser quel port est configuré sur l'OAW pour le service NOE:

```
(OAW-Master) (config) #show running-config | include "alg noe"
Building Configuration...
netservice svc-noe udp 32512 alg noe
netservice svc-noe-oxo udp 5000 alg noe
```

Pour un système OmniPCX Enterprise, ce port de signalisation a comme valeur par défaut 32512 et peut être modifié si l'infrastructure l'exige. Par contre, pour un système OmniPCX Office, ce port de signalisation n'est pas modifiable et a comme valeur 5000.

Pour déclarer le service NOE sur le port souhaité :

```
(OAW-Master) (config) #netservice svc-noe udp 32518 alg noe
```

Dans cet exemple, le service NOE est déclaré pour un système OXE sur le port udp-32518.

4.2.3 Sécurité avec licence PEFNG

La licence **PEFNG** active la fonctionnalité firewall de l'OAW. Pour tirer bénéfice de cette fonctionnalité, créer des règles de filtrage afin de n'autoriser que le trafic nécessaire au fonctionnement des mobiles. L'ajout de la licence **PEFNG** crée le rôle **voice**, cependant celui-ci est à compléter s'il est utilisé, la liste de règles ci-dessous reste la liste exhaustive.

Déclaration de l'objet **CS_voip** qui est la carte VoIP ou la GD du call server:

```
(OAW-Master) (config) #netdestination CS_voip
(OAW-Master) (config-dest) #host 192.168.20.6
```

Déclaration de l'objet **syslg_srv** qui est le PC permettant de récupérer les messages syslogs des postes à l'aide d'un serveur syslogs:

```
(OAW-Master) (config) #netdestination syslog_server
(OAW-Master) (config-dest) #host 192.168.30.10
```

Création des règles de sécurité:

```
(OAW-Master) (config) #ip access-list session MIPT_WMM_Rules
(OAW-Master) (config-sess-IPT-OT_WMM_Rules)#any any svc-dhcp permit
(OAW-Master) (config-sess-IPT-OT_WMM_Rules)#any any svc-icmp permit
(OAW-Master) (config-sess-IPT-OT_WMM_Rules)#user alias CS_voip svc-tftp permit
```

Sur OXE, utiliser le port svc-noe configuré pour correspondre à la configuration du système:

```
(OAW-Master) (config-sess-IPT-OT_WMM_Rules)#any any svc-noe permit queue high
```

Sur OXO, utiliser le port prédéfini svc-noe-oxo:

```
(OAW-Master) (config-sess-IPT-OT_WMM_Rules)#any any svc-noe-oxo permit queue high
```

```
(OAW-Master) (config-sess-IPT-OT_WMM_Rules)#user alias syslg_srv svc-syslog permit
(OAW-Master) (config-sess-IPT-OT_WMM_Rules)#user host 224.0.1.116 any permit
(OAW-Master) (config-sess-IPT-OT_WMM_Rules)#!
```

La règle de sécurité **`user host 224.0.1.116 any permit`** permet le multicast pour la fonction *push-to-talk* du call server et concerne uniquement l'OmniPCX Enterprise.

4.2.4 Création du rôle

Créer le rôle **`IPT-OT_WMM`** qui contient le filtre de sécurité défini précédemment.

```
(OAW-Master) (config) #user-role IPT-OT_WMM
(OAW-Master) (config-role) #session-acl IPT-OT_WMM_Rules
(OAW-Master) (config) #!
```

4.2.5 Attribution du rôle au client

Lorsqu'un poste s'associe à un AP, il reçoit son rôle initial, par défaut le rôle **`logon`**. Il convient de dériver le rôle **`logon`** vers le rôle **`IPT-OT_WMM`** créé précédemment : en choisissant une méthode d'authentification (authentification SSID ou authentification MAC par exemple). Les règles de sécurités associées seront appliquées au poste.

Dans cet exemple, le rôle sera dérivé en fonction de l'appartenance des postes au SSID "phone" en suivant les règles des "User Rules".

```
(OAW-Master) (config) #aaa derivation-rules user "IPT-OT"
(OAW-Master) (user-rule) #set role condition essid equals "phone" set-value "IPT-
OT_WMM" position 1
(OAW-Master) (user-rule) # !
```

Cette règle de dérivation doit être utilisée dans le profil d'authentification des mobiles.

```
(OAW-Master) (config) #aaa profile aaa_phone
(OAW-Master) (AAA Profile "aaa_phone") #user-derivation-rules IPT-OT
(OAW-Master) (AAA Profile "aaa_phone") #!
```

4.2.6 Firewall session-idle-timeout

Afin que la session de signalisation NOE soit toujours ouverte au niveau du firewall de l'OAW, il est nécessaire d'augmenter la valeur par défaut de la durée de vie des sessions.

```
(OAW-Master) (config) #firewall session-idle-timeout 30
```

4.3 AP virtuel

Créer l'AP virtuel qui diffusera le SSID "phone" et utilisera le profil d'authentification précédemment défini :

```
(OAW-Master) (config) #wlan virtual-ap phone
(OAW-Master) (Virtual AP profile "phone") #aaa-profile aaa_phone
(OAW-Master) (Virtual AP profile "phone") #ssid-profile ssid_phone_wpa2
(OAW-Master) (Virtual AP profile "phone") #vlan 20
(OAW-Master) (Virtual AP profile "phone") #no mobile-ip
(OAW-Master) (Virtual AP profile "phone") #!
```

4.4 Groupe d'AP

Attribuer au groupe d'AP "default" l'AP virtuel créé au paragraphe 4.3. La valeur par défaut des autres paramètres est conservée.

```
(OAW-Master) (config) #ap-group default
(OAW-Master) (AP group "default") #virtual-ap phone
(OAW-Master) (AP group "default") #no virtual-ap default
(OAW-Master) (AP group "default") #!
```

4.5 Proxy ARP

Avec cette fonctionnalité de proxy arp, l'OAW transforme les requêtes ARP multicast en unicast et les transmet au destinataire. Cela protège les terminaux voix des requêtes ARP intempestives et contribue à la stabilité de la solution. Dans le profil virtual AP, activer "Drop Broadcast and Multicast" et "Convert Broadcast ARP requests to unicast".

Cette fonctionnalité doit être activée.

```
(OAW-Master) (config) #wlan virtual-ap "phone"
(OAW-Master) (Virtual AP profile "phone") #broadcast-filter all
(OAW-Master) (Virtual AP profile "phone") #broadcast-filter arp
```

4.6 Configuration Radio

4.6.1 Utilisation de la radio 802.11a par les postes WLAN

La bande radio 802.11b/g est facilement interférée par d'autres périphériques, par exemple Bluetooth, caméras numériques Wi-Fi... Si possible, il est recommandé d'éviter d'utiliser cette radio et de choisir la bande 802.11a band pour les clients voix.

Les canaux DFS peuvent être utilisés mais si le contrôleur détecte la présence de radar ou de tout autre équipement prioritaire, tous les APs utilisant des canaux DFS devront changer de canal. Les logs permettant de voir la présence de radar se trouvent dans le guide de dépannage.

Note: si l'utilisation de canaux DFS est nécessaire pour le roaming en 802.11a, les performances peuvent se voire dégradées lors du scan passif des canaux. En 802.11a/n, les performances sont moindres lorsque plus de 8 canaux sont autorisés pour le roaming.

Pour utiliser les canaux DFS, il faut **activer** "Advertise 802.11d and 802.11h Capabilities" dans le profil 802.11a radio (voir section 4.6.4 Paramétrage des fréquences Radio).

Il est recommandé d'éviter l'utilisation de canaux DFS si possible.

Les canaux recommandés pour l'utilisation des IP Touch et OmniTouch WLAN sont :

- Pour le 802.11a : canaux 36, 40, 44 et 48 (canaux non DFS)
- Pour le 802.11b/g : canaux 1, 6 et 11 (canaux qui ne se chevauchent pas)

Autoriser uniquement les canaux non DFS (dépend du domaine de régulation):

```
(OAW-Master) (config) #ap regulatory-domain-profile default
(OAW-Master) (Regulatory Domain profile "default") #country-code FR
(OAW-Master) (Regulatory Domain profile "default") #valid-11g-channel 1
(OAW-Master) (Regulatory Domain profile "default") #valid-11g-channel 6
(OAW-Master) (Regulatory Domain profile "default") #valid-11g-channel 11

(OAW-Master) (Regulatory Domain profile "default") #valid-11a-channel 36
(OAW-Master) (Regulatory Domain profile "default") #valid-11a-channel 40
(OAW-Master) (Regulatory Domain profile "default") #valid-11a-channel 44
(OAW-Master) (Regulatory Domain profile "default") #valid-11a-channel 48
(OAW-Master) (Regulatory Domain profile "default") #no valid-11a-channel 52
(OAW-Master) (Regulatory Domain profile "default") #no valid-11a-channel 56
(OAW-Master) (Regulatory Domain profile "default") #no valid-11a-channel 60
(OAW-Master) (Regulatory Domain profile "default") #no valid-11a-channel 64
(OAW-Master) (Regulatory Domain profile "default") #no valid-11a-channel 100
(OAW-Master) (Regulatory Domain profile "default") #no valid-11a-channel 104
(OAW-Master) (Regulatory Domain profile "default") #no valid-11a-channel 108
(OAW-Master) (Regulatory Domain profile "default") #no valid-11a-channel 112
(OAW-Master) (Regulatory Domain profile "default") #no valid-11a-channel 116
(OAW-Master) (Regulatory Domain profile "default") #no valid-11a-channel 120
(OAW-Master) (Regulatory Domain profile "default") #no valid-11a-channel 124
(OAW-Master) (Regulatory Domain profile "default") #no valid-11a-channel 128
(OAW-Master) (Regulatory Domain profile "default") #no valid-11a-channel 132
(OAW-Master) (Regulatory Domain profile "default") #no valid-11a-channel 136
(OAW-Master) (Regulatory Domain profile "default") #no valid-11a-channel 140
```

4.6.2 ARM – Adaptive Radio Management

La fonction Automatic Radio Management peut être utilisée pour avoir une configuration automatique des APs (canal, puissance de transmission…). Tous les APs passent en monitoring pendant 110 ms toutes les 10s. Cette fonctionnalité ne doit pas s'enclencher alors qu'un utilisateur est en communication (voip-aware-scan).

```
(OAW-Master) (config) #rf arm-profile "Aware_ARM"
(OAW-Master) (Adaptive Radio Management (ARM) profile "Aware_ARM")#min-tx-power 18
(OAW-Master) (Adaptive Radio Management (ARM) profile "Aware_ARM")#no multi-band-scan
(OAW-Master) (Adaptive Radio Management (ARM) profile "Aware_ARM")#voip-aware-scan
(OAW-Master) (Adaptive Radio Management (ARM) profile "Aware_ARM")#no ps-aware-scan
(OAW-Master) (Adaptive Radio Management (ARM) profile "Aware_ARM")#!

(OAW-Master) (config) #rf dot11a-radio-profile "default"
(OAW-Master) (802.11a radio profile "default") #arm-profile "Aware_ARM"
(OAW-Master) (802.11a radio profile "default") #!
(OAW-Master) (config) #rf dot11g-radio-profile "default"
(OAW-Master) (802.11g radio profile "default") #arm-profile "Aware_ARM"
(OAW-Master) (802.11g radio profile "default") #!
(OAW-Master) (config) #rf optimization-profile "default"
(OAW-Master) (RF Optimization Profile "default") #no handoff-assist
```

4.6.3 ARM et Basic & Transmit rates optimisation

Le service ARM pouvant entraîner une diminution de la bande passante et des problèmes de voix, il est parfois judicieux de désactiver la fonctionnalité après quelques temps de calcul initial.

La désactivation de l'ARM est recommandée si la couverture radio semble faible ou si des resets dus à des "UDP Lost" apparaissent. Il est possible de garder les paramètres calculés pendant que cette fonction était active, en positionnant l'ARM en mode "maintain" :

```
(OAW-Master) (config) #rf arm-profile "Aware_ARM"
(OAW-Master) (Adaptive Radio Management (ARM) profile "Aware_ARM")#assignment maintain
(OAW-Master) (Adaptive Radio Management (ARM) profile "Aware_ARM")#no scanning
(OAW-Master) (Adaptive Radio Management (ARM) profile "Aware_ARM")#!
```

Le délai minimum pour une bonne configuration des APs grâce à l'ARM est de 1 jour.

```
(OAW-Master) #show rf arm-profile "Aware_ARM"
Adaptive Radio Management (ARM) profile "Aware_ARM"
-------------------------------------------------
Parameter                          Value
---------                          -----
Assignment                         maintain
Allowed bands for 40MHz channels   a-only
Client Aware                       Enabled
Max Tx Power                       30 dBm
Min Tx Power                       17 dBm
Multi Band Scan                    Disabled
Rogue AP Aware                     Disabled
Scan Interval                      10 sec
Scanning                           Disabled
Scan Time                          110 msec
VoIP Aware Scan                    Enabled
Power Save Aware Scan              Disabled
Ideal Coverage Index               10
Acceptable Coverage Index          4
Wait Time                          15 sec
Free Channel Index                 25
Backoff Time                       240 sec
Error Rate Threshold               50 %
Error Rate Wait Time               30 sec
Noise Threshold                    75 -dBm
Noise Wait Time                    120 sec
Minimum Scan Time                  8 sec
Load aware Scan Threshold          1250000 Bps
Mode Aware Arm                     Disabled
```

Noter que pour de meilleures performances et une qualité de déploiement optimales, il est recommandé de positionner l'ARM "Assignment" à "disable" et d'effectuer une planification manuelle des canaux suivant une étude de couverture professionnelle orientée pour un déploiement voix.

```
(OAW-Master) (config) #rf arm-profile "No_ARM"
(OAW-Master) (Adaptive Radio Management (ARM) profile "No_ARM")#assignment disable
```

Dans cet exemple, le canal utilisé est le 40 avec une puissance d'émission de 30 dBm pour la radio 802.11a et le canal 11 pour la bande 802.11b/g. Ces valeurs doivent être adaptées à l'utilisation sur site. Se référer aux Règles d'Ingénieries.

```
(OAW-Master) (config) #rf dot11a-radio-profile "default"
(OAW-Master) (802.11a radio profile "default") #channel 40
(OAW-Master) (802.11a radio profile "default") #tx-power 30
(OAW-Master) (802.11a radio profile "default") #arm-profile "No_ARM"
(OAW-Master) (802.11a radio profile "default") #!

(OAW-Master) (config) #rf dot11g-radio-profile "default"
(OAW-Master) (802.11g radio profile "default") #channel 1
(OAW-Master) (802.11g radio profile "default") #tx-power 30
(OAW-Master) (802.11g radio profile "default") #arm-profile "No_ARM"
(OAW-Master) (802.11g radio profile "default") #!
```

En 802.11b/g/n, utiliser uniquement les canaux 1, 6 et 11. En 802.11a/n, utiliser les canaux selon les règles notes dans le guide de l'OAW et conformément au domaine de régulation local.

Si une bonne couverture radio est constatée pour la voix ou que plusieurs SSIDs sont utilisés, la désactivation des transmissions 1 et 2 Mbps permet d'améliorer la qualité de la voix.

```
(OAW-Master) (config) #wlan ssid-profile ssid_phone_wpa2
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #no g-basic-rates
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #g-basic-rates 6 11
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #no g-tx-rates
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #g-tx-rates 6 12 18 24 36 48 54
(OAW-Master) (SSID Profile "ssid_phone_wpa2") #!
```

Note: afin d'optimiser les performances, il est recommandé de refuser que les clients 802.11b s'associent en configurant les débits 6 Mbps ou 12 Mbps comme obligatoire dans la configuration 802.11g.

4.6.4 Paramétrage des fréquences Radio

Les postes OmniTouch 81x8 utilisent le mode par défaut "World mode regulatory domain" qui est "World Mode (802.11d)". Ce mode 802.11d nécessite que l'infrastructure diffuse ces capacités 802.11d et 802.11h, sinon les modes ETSI, USA ou Japan doivent être sélectionnés localement sur les postes OmniTouch.

Pour configurer le world mode sur le switch: activer "Advertise 802.11d and 802.11h Capabilities", activer "Enable CSA" et positionner l'intervalle entre deux beacons à 100:

```
(OAW-Master) (config) #rf dot11a-radio-profile "default"
(OAW-Master) (802.11a radio profile "default") #dot11h
(OAW-Master) (802.11a radio profile "default") #csa
(OAW-Master) (802.11a radio profile "default") #beacon-period 100
(OAW-Master) (802.11a radio profile "default") #arm-profile "No_ARM"
(OAW-Master) (802.11a radio profile "default") #!

(OAW-Master) (config) #rf dot11g-radio-profile "default"
(OAW-Master) (802.11a radio profile "default") #dot11h
(OAW-Master) (802.11a radio profile "default") #csa
(OAW-Master) (802.11a radio profile "default") #beacon-period 100
(OAW-Master) (802.11g radio profile "default") #arm-profile "No_ARM"
(OAW-Master) (802.11g radio profile "default") #!
```

5. CONFIGURATION DES POINTS D'ACCES

A partir de la version 3.1, les APs n'utilisent plus le "Location ID" mais appartiennent à un groupe. Le nom du groupe est inscrit dans les variables d'environnement de l'AP. Le groupe d'appartenance par défaut est le groupe "Default". Dans l'exemple, le groupe "Default" est utilisé.

5.1 Configuration du serveur DHCP de l'OAW

La configuration IP des APs peut être faite en statique ou dynamique à travers un serveur DHCP.

Note: le serveur DHCP embarqué sur l'OAW ne permet pas de configurer tous les paramètres nécessaires au démarrage des postes IP Touch et OmniTouch WLAN en mode dynamique. Un serveur DHCP dédié doit être utilisé à la place.

Dans cet exemple, le serveur DHCP embarqué dans l'OAW est utilisé pour fournir les paramètres IP aux Aps, appartenant au VLAN 10. La plage IP allouée aux APs va de 192.168.10.3 à 192.168.10.9.

```
(OAW-Master) (config) #ip dhcp pool AP
(OAW-Master) (config-dhcp)#network 192.168.10.0 /24
(OAW-Master) (config-dhcp)#default-router 192.168.10.1
(OAW-Master) (config-dhcp)#!
(OAW-Master) (config) #ip dhcp excluded-address 192.168.10.1 192.168.10.2
(OAW-Master) (config) #ip dhcp excluded-address 192.168.10.10 192.168.10.255
(OAW-Master) (config) #!
(OAW-Master) (config) #service dhcp
```

Pour visualiser la configuration DHCP :

```
(OAW-Master) #show ip dhcp database

DHCP enabled

# AP
subnet 192.168.10.0 netmask 255.255.255.0 {
        default-lease-time 172800;
        max-lease-time 172800;
        option vendor-class-identifier  "ArubaAP";
        option vendor-encapsulated-options  "192.168.10.2";
        option routers 192.168.10.1;
        range 192.168.10.3 192.168.10.9;
        authoritative;
}
```

Si un AP est directement connecté sur un port de l'OAW, le port devra être configuré en mode "Access" du VLAN 10. Par exemple, pour connecter un AP sur le port 0 de l'OAW, la configuration se fait comme suit :

```
(OAW-Master) (config) #interface fastethernet 1/0
(OAW-Master) (config-if)#switchport mode access
(OAW-Master) (config-if)#switchport access vlan 10
(OAW-Master) (config-if)#!
```

5.2 Réinitialisation d'un AP

S'il s'avère nécessaire de réinitialiser un AP à ses paramètres d'usine (en raison de variables d'environnement positionnées lors d'une précédente installation et incompatibles avec la nouvelle), la procédure est la suivante :

- Activer le "Serial over Ethernet" au niveau de l'OAW

```
(OAW-Master) (config) #telnet soe
```

Note
Vérifier le matériel utilisé, la fonction telnet SOE n'est plus disponible avec les nouveaux hardwares. Pour formater un AP, il faut utiliser soit le port série sur l'AP (si disponible) soit un adaptateur série pour AP.

- Pour les anciens contrôleurs, connecter l'AP sur le contrôleur et réaliser un telnet vers le port 2300 du contrôleur. Dans cet exemple, l'AP est connecté sur le port 0 (slot 1/port 0).
- Pour les nouveaux contrôleurs, utiliser HyperTerminal.

```
> telnet 192.168.10.2 2300

User: admin
Password: admin
Available commands:
  connect <slot/port>
  exit (no args)
soe> connect 1/0
Connecting to 1/0 at 9600 baud 8N1
Type "~." to disconnect
```

- Débrancher/rebrancher l'AP et presser ***<Enter>*** au message ***Hit <Enter> to stop autoboot:3*** pour entrer en ligne de commande sur l'AP. Taper ***Enter*** rapidement car il n'y a que quelques secondes pour accéder à la ligne de commande.

```
Hit <Enter> to stop autoboot:  0
apboot>
```

- Si la configuration de l'AP n'est pas vierge, il faut remettre à zéro tous les paramètres de configuration.

```
apboot> purgeenv
apboot> save
Erasing....
Programming....
Verifying....
apboot> reset
```

L'AP redémarrera, obtiendra les paramètres IP configurés au niveau du serveur DHCP de l'OAW, se connectera à l'OAW et prendra les paramètres WLAN du groupe "Default".

6. RAPPEL SUR LA QOS DES OmniPCX

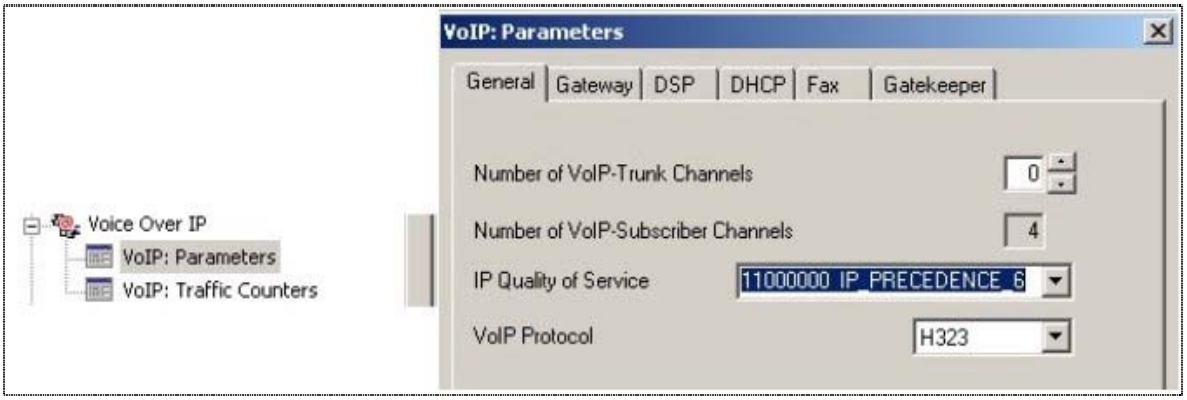
Suivant la configuration du menu admin, les postes WLAN peuvent utiliser les priorités :

- Configurées dans le menu admin
- Configuré sur le PCX dans les paramètres "Qualité de Service IP".

6.1 Configuration OmniPCX Office

Dans **`OMC > Paramètres VoIP`**, configurer le paramètre **`Qualité de Service IP`**.

Ce paramètre prend une valeur comprise entre 0 et 7 (0 signifiant pas de priorité et 7 donnant la priorité maximum pour le trafic).



6.2 Configuration OmniPCX Enterprise

Dans mgr sur l'OXE, **`IP > Descendre dans la hiérarchie > Catégorie de qualité de service IP`**.

Plus la valeur pour le timer **`UDP Lost`** est élevée, plus le temps pour détecter une perte de CS ou d'OAW sera important, moins il y aura de resets de postes WLAN. Cela dépend des besoins et de la topologie.

```
┌─Consultation/Modification: Catégorie de qualité de service IP─┐
│                                                               │
│     No noeud-réseau (réservé soft) : 1                        │
│           Instance (réservée soft) : 1                        │
│    No Catégorie Qualité Service IP : 1                        │
│                                                               │
│   Nom Catégorie Qualité de Service : --------------------     │
│              Utilisation de 802.1Q + Non                      │
│                    Priorite 802.1p : 5                        │
│                            VLAN ID : 0                        │
│                       TOS/diffServ : 46                       │
│                           UDP Lost : 60                       │
│                     UDP Lost Reinit : 15                      │
│                      UDP Keep Alive : 15                      │
│                  Diff. service SIP : 40                       │
│                  SIP Diff. Service : 40                       │
│                           SIP Lost : 5                        │
│                      SIP Keep Alive : 30                      │
│                                                               │
└───────────────────────────────────────────────────────────────┘
```

7. AVERTISSEMENT

Alcatel-Lucent n'est pas tenu responsable des choix de paramétrages client qui n'ont pas été préconisés dans ses communications.